PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-056963
(43)Date of publication of application : 25.02.2000

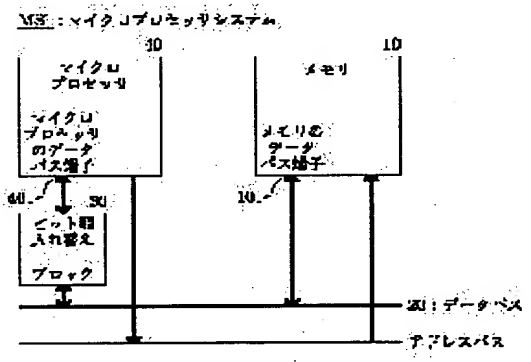
(51)Int.Cl. G06F 9/06
G06F 12/14
G06K 19/073

(21)Application number : 10-235034
(22)Date of filing : 06.08.1998

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : URANO MASAMI

(54) MICRO PROCESSOR SYSTEM, MICRO PROCESSOR OPERATION ANALYSIS PREVENTING METHOD, AND RECORDING MEDIUM RECORDED WITH MICRO PROCESSOR OPERATION ANALYSIS PREVENTING PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a micro processor system by which the analysis of a program on a memory and a bus is difficult so that the operation of the micro processor is not analyzed even if the program is read, and to provide a micro processor operation analysis preventing method and a recording medium in which a micro processor operation analysis preventing program is recorded.
SOLUTION: This system is constituted of a micro processor 40, a memory 10 preserving at least a program or data which can be executed by the micro processor 40, and address bus/data bus 20 connecting the micro processor 40 to the memory 10. The bit order of the terminal of the data bus 20 of the micro processor 40 and the bit order of the terminal of the data bus 20 of the memory 10 are changed.



LEGAL STATUS

[Date of request for examination] 22.01.2001
[Date of sending the examiner's decision of rejection] 21.05.2004
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－56963
（Ｐ2000－56963Ａ）
(43)公開日　平成12年２月25日(2000.2.25)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'（参考）
Ｇ０６Ｆ　9/06	５５０	Ｃ０６Ｆ　9/06	５５０Ｂ	５Ｂ０１７
12/14	３２０	12/14	３２０Ｂ	５Ｂ０３５
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	５Ｂ０７６

審査請求　未請求　請求項の数12　ＦＤ　（全 15 頁）

(21)出願番号　特願平10－235034

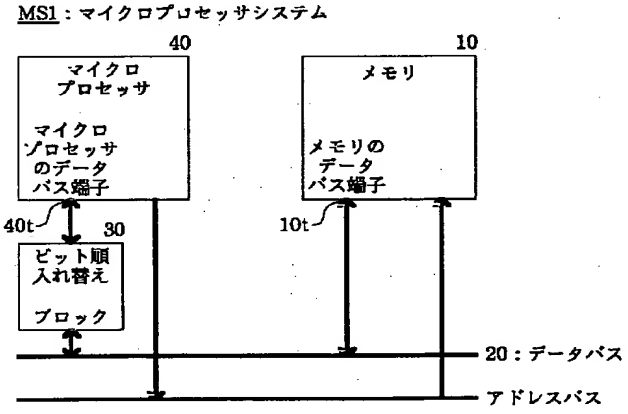
(22)出願日　平成10年８月６日(1998.8.6)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　浦野　正美
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内
(74)代理人　10008/446
弁理士　川久保　新一

Ｆターム(参考)　5B017 AA07 BA07 CA04
5B035 AA13 BB09 CA38
5B076 FA02

(54)【発明の名称】　マイクロプロセッサシステム、マイクロプロセッサ動作解析防止方法およびマイクロプロセッサ動作解析防止プログラムを記録した記録媒体

(57)【要約】
【課題】　プログラムを読み取られても、マイクロプロセッサの動作を解析されないように、メモリ上およびバス上のプログラムの解析が困難であるマイクロプロセッサシステム、マイクロプロセッサ動作解析防止方法およびマイクロプロセッサ動作解析防止プログラムを記録した記録媒体を提供するものである。
【解決手段】　マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているシステムにおいて、上記マイクロプロセッサのデータバスの端子のビット順と上記メモリのデータバスの端子のビット順とを変えるものである。



【特許請求の範囲】
【請求項１】　マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているマイクロプロセッサシステムにおいて、
上記マイクロプロセッサが処理する上記データまたは上記プログラムのビット順と、上記メモリに格納されている上記データまたは上記プログラムのビット順とを異ならせることを特徴とするマイクロプロセッサ動作解析防止方法。
【請求項２】　請求項１において、
上記メモリに格納されている上記データまたは上記プログラムの同一ワード内におけるビット順を入れ換えることによって、上記マイクロプロセッサが処理する上記データまたは上記プログラムのビット順と同一になることを特徴とするマイクロプロセッサ動作解析防止方法。
【請求項３】　請求項１において、
上記マイクロプロセッサに接続されている第１のメタル配線と、上記メモリに接続されている第２のメタル配線と、上記第１のメタル配線と上記第２のメタル配線との相互間に接続されているＭＯＳトランジスタと、上記ＭＯＳトランジスタのゲートを制御する制御手段とによってビット順入れ換えブロックが構成され、上記ＭＯＳトランジスタのゲートに所望の制御信号を与えることによって、ビット順を入れ換えることを特徴とするマイクロプロセッサ動作解析防止方法。
【請求項４】　請求項１において、
上記メモリのデータバス端子と上記マイクロプロセッサのデータバス端子との接続順に基づいて、上記マイクロプロセッサのプログラムの各ワード内のビット順を変更することを特徴とするマイクロプロセッサ動作解析防止方法。
【請求項５】　ビット順変換前のデータまたはプログラムを所定バイト、読み込む読み込み手順と；上記読み込んだ所定バイトの中でビット位置の入れ換えを行うビット位置入れ換え手順と；上記ビット位置の入れ換えが行われたデータまたはプログラムを書き出す書き出し手順と；をコンピュータに実行させるマイクロプロセッサ動作解析防止プログラムが記録されているコンピュータ読み取り可能な記録媒体。
【請求項６】　マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているマイクロプロセッサシステムにおいて、
上記マイクロプロセッサが処理するプログラム、データのうちの少なくとも一方のビット順と、上記メモリに格納されているプログラム、データのうちの少なくとも一方のビット順とを異ならせるビット順入れ換えブロックを有することを特徴とするマイクロプロセッサシステム。
【請求項７】　請求項６において、
上記ビット順入れ換えブロックは、上記マイクロプロセッサのデータバス端子と上記データバスとの間の領域、または、マイクロプロセッサコアとマイクロプロセッサのデータバス端子との間の領域に設けられていることを特徴とするマイクロプロセッサシステム。
【請求項８】　請求項６において、
上記メモリは、上記ビット順入れ換えブロックによって、ワード内のビットが入れ換えられたプログラム、データのうちの少なくとも一方を格納するメモリであることを特徴とするマイクロプロセッサシステム。
【請求項９】　請求項６において、
上記ビット順入れ換えブロックは、
上記マイクロプロセッサに接続されている第１のメタル配線と；上記メモリに接続されている第２のメタル配線と；上記第１のメタル配線の所定部分と上記第２のメタル配線の所定部分とを接続するスルーホールと；を有するブロックであることを特徴とするマイクロプロセッサシステム。
【請求項１０】　請求項６において、
上記ビット順入れ換えブロックは、
上記マイクロプロセッサに接続されている第１のメタル配線と；上記メモリに接続されている第２のメタル配線と；上記第１のメタル配線と上記第２のメタル配線との相互間に接続されているＭＯＳトランジスタと；上記ＭＯＳトランジスタのゲートを制御する制御手段と；を有し、上記ＭＯＳトランジスタのゲートに所望の制御信号を与えることによって、ビット順を入れ換えるブロックであることを特徴とするマイクロプロセッサシステム。
【請求項１１】　請求項１０において、
上記制御信号は、上記メモリの所定のワード内の所定のビットに格納されていることを特徴とするマイクロプロセッサシステム。
【請求項１２】　請求項６において、
上記メモリに格納されているプログラムまたはデータは、同一ワード内のビット順を入れ換えることができるプログラムによって生成されたものか、または上記ビット順を入れ換えることができる機能を持つプログラムによって、上記メモリ上にロードされているものであることを特徴とするマイクロプロセッサシステム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ＩＣカード等に用いるマイクロプロセッサに関するものである。
【０００２】
【従来の技術】図１９は、従来のマイクロプロセッサシ

ステムＭＳの構成の一例を示す図である。

【０００３】ここでは、８ビットのマイクロプロセッサであるＺ８０を例にとって説明するが、さらに多ビットのマイクロプロセッサを使用した場合も、上記の場合と同様に考えることができる。

【０００４】従来のマイクロプロセッサシステムＭＳは、マイクロプロセッサ４とメモリ１とによって構成され、マイクロプロセッサ４のアドレスバス端子とメモリ１のアドレスバス端子とがアドレスバスによって接続され、マイクロプロセッサ４のデータバス端子４ｔとメモリ１のデータバス端子１ｔとがデータバス２によって接続されている。

【０００５】図２０は、上記従来例におけるマイクロプロセッサのデータバス端子とメモリのデータバス端子との接続を示す図である。

【０００６】上記従来例において、マイクロプロセッサ４側のデータバス２のＭＳＢの配線Ｄ７とメモリ１側のデータバスのＭＳＢの配線Ｄ７とが接続されている。配線Ｄ６、Ｄ５、…Ｄ０のそれぞれも、上記と同様に、同じビット順同士が接続されている。

【０００７】図２１は、従来例におけるメモリ１の内容を示す図である。

【０００８】マイクロプロセッサ４が実行するプログラムは、図２１に示すように、メモリ１中に保存され、ここでは、８ビットマイクロプロセッサ４であるＺ８０を例にとって説明するが、他のマイクロプロセッサでも、上記と同様である。

【０００９】ここに示した例では、０番地に１６進数で３１（以下、１６進数で示す）（００１１０００１）、１番地にＦＦ、２番地に７Ｆ、３番地に０６等が格納されている。また、４番地以降にも、上記と同様に、プログラムが格納されている。これらは、Ｚ８０の機械語では、ＬＤ　ＳＰ，７ＦＦＦ、ＬＤ　Ｂ，１１等を示している。

【００１０】マイクロプロセッサ４がリセット信号によりリセットされ、次にリセットが解除されると、マイクロプロセッサ４はアドレスバスに０を出力する。このデータをアドレスとして、メモリ１がその０番地の内容３１をデータバス２に出力すると、マイクロプロセッサ４は、そのデータを内部に取り込んでデコードし、さらにオペランドを取得するために、１、２をアドレスバスに出力し、それぞれの番地の内容のＦＦ、７Ｆをメモリ１から読み出す。

【００１１】マイクロプロセッサ４は、これらの読み出されたデータをＬＤ　ＳＰ，７ＦＦＦという命令であると解釈し、自分自身のＳＰに７ＦＦＦを設定する。その後、次の命令を取得するために、４をアドレスバスに出力し、メモリ１の４番地の内容の０６を読み出す。以上のようにして、マイクロプロセッサ４は順次アドレスを出力し、メモリ１の該当する番地の内容を読み出して命令を実行していく。

【００１２】上記のように、従来のマイクロプロセッサ４では、データバス２を介して、メモリ１の内容を順次読み出し、その値をマイクロプロセッサ４内部で解釈し、そのデータに対応する命令を順次実行する。プログラム自体は、実行する順番で、メモリ１上に格納されている。また、各番地には、プログラムの各ステップの命令コードが格納され、メモリ１のＭＳＢ側（ここではビット７とする）に命令コードのＭＳＢ（ビット７）が格納され、メモリ１のビット６には命令コードのビット６が格納され、同様に、ＬＳＢまで順番に格納されている。

【００１３】ところで、近年ＩＣカードの応用分野が拡大しつつあるが、これにつれてＩＣカードのセキュリティの問題が重視されている。ＩＣカード内に納められている機密情報を解読しようとする場合、マイクロプロセッサ４の論理回路、プログラムを容易に解読することができると、この情報を元に内部を解析し、機密情報を解読される可能性がある。

【００１４】

【発明が解決しようとする課題】従来のマイクロプロセッサ４のように、プログラムがメモリ１上に順番に、かつ各ワード内でもビット順に格納されている場合、該当するメモリセルのデータを順番に読み取ることによってプログラムが容易に解読される可能性がある。

【００１５】また、上記のように、プログラムはメモリ１からデータバス２を介してマイクロプロセッサ４に送られ、この場合、メモリ１のデータを解析しなくても、データバス２を観測することによって、プログラムを順次読み取ることができ、これをもとに動作を容易に解析される可能性がある。

【００１６】本発明は、プログラムを読み取られても、マイクロプロセッサの動作を解析されないように、メモリ上およびバス上のプログラムの解析が困難であるマイクロプロセッサシステム、マイクロプロセッサ動作解析防止方法およびマイクロプロセッサ動作解析防止プログラムを記録した記録媒体を提供するものである。

【００１７】

【課題を解決するための手段】本発明は、マイクロプロセッサと、上記マイクロプロセッサで実行可能なプログラム、データのうちの少なくとも一方を保存するメモリと、上記マイクロプロセッサと上記メモリとを接続するアドレスバスとデータバスとによって構成されているシステムにおいて、上記マイクロプロセッサのデータバスの端子のビット順と上記メモリのデータバスの端子のビット順とを変えるものである。

【００１８】

【発明の実施の形態および実施例】図１は、本発明の第１の実施例であるマイクロプロセッサシステムＭＳ１を示す図である。

【００１９】マイクロプロセッサシステムＭＳ１は、基本的には、従来例と同様のシステムであるが、データバス２０とマイクロプロセッサ４０のデータバス端子４０ｔとの間に、ビット順入れ換えブロック３０が接続されている点が、上記従来例とは異なる。

【００２０】メモリ１０側において、データバス２０の各ビットが、従来例と同様に、メモリ１０のデータバス端子１０ｔの同じビットに順番に接続されている。また、マイクロプロセッサ４０のアドレスバスの端子におけるビット順と、メモリ１０のアドレスバスの端子におけるビット順とは、同じ順序で接続されている。つまり、アドレスに関して、ビット順入れ換えブロックが設けられていない。

【００２１】図２は、上記実施例におけるビット順入れ換えブロック３０の具体例を示す図である。

【００２２】図２に示す例では、ビット順入れ換えブロック３０によって、マイクロプロセッサ４０のデータバス端子４０ｔ側の配線Ｄ７をメモリ１０のデータバス端子１０ｔ側の配線Ｄ５へ入れ換え、以下それぞれ、Ｄ６をＤ２へ、Ｄ５をＤ１へ、Ｄ４をＤ６へ、Ｄ３をＤ０へ、Ｄ２をＤ４へ、Ｄ１をＤ３へ、Ｄ０をＤ７へ入れ換えて接続している。

【００２３】なお、図２では、１種類の接続法が記載されいるが、データバス２０の各ビットと、マイクロプロセッサ４０のデータバス端子４０ｔの各ビットとを、１：１に接続するものであれば、図２に示すブロック３０における接続法以外の接続法を採用するようにしてもよい。

【００２４】図３は、上記実施例におけるメモリ１０に格納すべきデータの例を示す図である。

【００２５】上記実施例では、メモリ１０のデータバス端子１０ｔのビット順と、マイクロプロセッサ４０のデータバス端子４０ｔのビット順とが互いに異なるので、従来と同様の命令コードをメモリ１０に格納しても、マイクロプロセッサ４０が正常には動作しない。

【００２６】つまり、メモリ１０の０番地に、従来例と同様に、たとえば、３１（００１００００１）を格納しても、ビット順入れ換えブロック３０によって、データが入れ換えられ、マイクロプロセッサ４０のデータバス端子４０ｔでは８Ｃ（１０００１０００）になり、マイクロプロセッサ４０は、これをＡＤＣ　Ａ，Ｈという命令と解釈する。したがって、正常に動作させるためには、命令コードのビット順を予め入れ換えた後に、メモリ１０に格納する必要がある。この場合、０番地にデータＣ２を格納し、１番地にデータＦＦを格納し、２番地にデータＤＦを格納し、以下各番地に、データ１８、Ｃ０、１９、０Ａ、８８、Ｂ４、Ｆ４を格納する。

【００２７】図４は、メモリ１０のデータバス端子１０ｔにおけるプログラムのビット順と、マイクロプロセッサ４０のデータバス端子４０ｔにおけるプログラムのビット順とが、どのように変換されているかを具体的に示す図である。

【００２８】メモリ１０のデータバス端子１０ｔに、０番地のデータとして、１０００００１０（Ｃ２）のデータが出力されたとすると、各ビットはビット順入れ換えブロック３０を介して、マイクロプロセッサ４０のデータバス端子４０ｔに到達し、その値はビット７から順番に００１００００１（３１）になり、ＬＤ　ＳＰ，ｎｎ（ｎｎは１６bit の値）という命令であり、この命令コードは、従来例における命令コードと同じ命令コードである。

【００２９】ここで、まず、元となるプログラムにおける各ワード内のビット順を予め入れ換え、このようにビット順を入れ換えたデータを、メモリ１０に格納しておく。マイクロプロセッサ４０が、従来例と同様に各番地のデータを順次読み出し、このデータ読み出し時に、メモリ１０のデータバス端子１０ｔや、データバス２０に出現するデータのビット順は、元のプログラムのビット順とは入れ替わっているので、データバス２０に出現するデータをマイクロプロセッサ４０がそのまま実行しても、元のプログラムと同じ動作をすることはできない。

【００３０】すなわち、第三者がメモリ１０の内容や、データバス２０の内容を何らかの方法で観測し、マイクロプロセッサ４０の動作を解析しようとしても、メモリ１０に格納されているデータや、データバス２０上のデータは、そのビット順が入れ換えられたデータであり、元のプログラムのビット順とは異なっているので、元のプログラムの動作を解析することは困難である。

【００３１】ところが、データバス２０に出現するデータが、ビット順入れ換えブロック３０を介して、マイクロプロセッサ４０のデータバス端子４０ｔに到達すると、ビット順入れ換えブロック３０で各ワード内のビット順が入れ換えられ、その後、マイクロプロセッサ４０に到達するので、マイクロプロセッサ４０のデータバス端子４０ｔでは元のプログラムと同じビット順になる。したがって、マイクロプロセッサ４０は元のプログラムと同じ動作を実行することができる。

【００３２】図５は、上記実施例におけるビット順入れ換えブロック３０の具体例を示す図である。

【００３３】ビット順入れ換えブロック３０は、１層メタル配線と２層メタル配線とを有し、１層メタル配線と２層メタル配線とが基板を挟んで配置されているブロックである。なお、図５において、１層メタル配線が水平に描かれ、２層メタル配線が垂直に描かれている。そして、データバス２０の各配線が１層メタル配線に接続され、マイクロプロセッサ４０のデータバス端子４０ｔに接続されている各配線が２層メタル配線に接続されている。

【００３４】そして、１層メタル配線の配線Ｄ７は、データバス２０の配線Ｄ７に接続され、１層メタル配線の

配線Ｄ６は、データバス２０の配線Ｄ６に接続され、以下、上記と同様に配線Ｄ０まで接続されている。また、２層メタル配線の配線Ｄ７は、マイクロプロセッサ４０のデータバス端子４０ｔの配線Ｄ７に接続され、２層メタル配線の配線Ｄ６は、マイクロプロセッサ４０のデータバス端子４０ｔの配線Ｄ６に接続され、以下、上記と同様に配線Ｄ０まで接続されている。

【００３５】そして、１層メタル配線と２層メタル配線とが絶縁性の基板を挟んで重なる場所のうちで、所定の場所にスルーホールを設け、このスルーホールによって１層メタル配線と２層メタル配線とが接続され、これによって、ビット順入れ換えを行う。

【００３６】つまり、ビット順入れ換えブロック３０において、２層メタル配線の配線Ｄ７と１層メタル配線の配線Ｄ５とが接続され、２層メタル配線の配線Ｄ６と１層メタル配線の配線Ｄ２とが接続され、２層メタル配線の配線Ｄ５と１層メタル配線の配線Ｄ１とが接続され、２層メタル配線の配線Ｄ４と１層メタル配線の配線Ｄ６とが接続され、２層メタル配線の配線Ｄ３と１層メタル配線の配線Ｄ０とが接続され、２層メタル配線の配線Ｄ２と１層メタル配線の配線Ｄ４とが接続され、２層メタル配線の配線Ｄ１と１層メタル配線の配線Ｄ３とが接続され、２層メタル配線の配線Ｄ０と１層メタル配線の配線Ｄ７とが接続されている。

【００３７】このように接続することによって、図４に示すビット順入れ換えブロック３０と同様なビット順の入れ換えが行われる。

【００３８】すなわち、ビット順入れ換えブロック３０は、マイクロプロセッサ４０に接続されている第１のメタル配線と、メモリ１０に接続されている第２のメタル配線と、上記第１のメタル配線の所定部分と上記第２のメタル配線の所定部分とを接続するスルーホールとを有するブロックである。

【００３９】なお、上記実施例は、１層メタル配線、２層メタル配線、１層メタル配線と２層メタル配線との間のスルーホールを用いた例であるが、これ以外の配線層を用いて、ビット毎に異なった配線を行うブロックを採用するようにしてもよい。

【００４０】図６は、ビット順入れ換えブロック３０の代わりに使用することができるビット順入れ換えブロック３０ａの構成を示す図である。

【００４１】ビット順入れ換えブロック３０ａは、ＮチャネルＭＯＳトランジスタによって、データバス２０の配線の１つと、マイクロプロセッサ４０のデータバス端子４０ｔの配線の１つとを接続するブロックである。

【００４２】つまり、図６に示す例では、マイクロプロセッサ４０側の配線Ｄ７とデータバス２０側の配線Ｄ７～Ｄ０のそれぞれとに、ＮチャネルＭＯＳトランジスタのソースとドレインとが接続されている。マイクロプロセッサ４０側の配線Ｄ６とデータバス２０側の配線Ｄ７～Ｄ０のそれぞれとに、上記と同様に、ＮチャネルＭＯＳトランジスタが接続されている。配線Ｄ５～Ｄ０のそれぞれについても、上記と同様に、ＮチャネルＭＯＳトランジスタが接続されている。

【００４３】そして、上記ＮチャネルＭＯＳトランジスタのうちの所定のＮチャネルＭＯＳトランジスタのゲート電極に０または１（制御信号）を印加する（すなわち、ＧＮＤまたはＶＤＤに接続する）。これによって、マイクロプロセッサ４０のデータバス端子４０ｔとデータバス２０との接続を行い、所定のビット順入れ換えを行う。

【００４４】この場合、Ｄ０－Ｄ７に１を印加し（マイクロプロセッサ４０側の配線Ｄ０とデータバス２０側の配線Ｄ７とを接続するＮチャネルＭＯＳトランジスタのゲート電極に１を印加し）、またＤ４－Ｄ６、Ｄ７－Ｄ５、Ｄ２－Ｄ４、Ｄ１－Ｄ３、Ｄ６－Ｄ２、Ｄ５－Ｄ１、Ｄ３－Ｄ０にも１を印加し（ＶＤＤに接続し）、その他に、０を印加する（ＧＮＤに接続する）。これによって、図４に示すビット順入れ換えブロック３０と同じビット順の入れ換えを行うことができる。

【００４５】つまり、ビット順入れ換えブロック３０ａは、マイクロプロセッサに接続されている第１のメタル配線と、上記メモリに接続されている第２のメタル配線と、上記第１のメタル配線と上記第２のメタル配線との相互間に接続されているＭＯＳトランジスタと、上記ＭＯＳトランジスタのゲートを制御する制御手段とを有し、上記ＭＯＳトランジスタのゲートに所望の制御信号を与えることによって、ビット順を入れ換えるビット順入れ換えブロックの例である。

【００４６】なお、ビット順入れ換えブロック３０ａでは、ＮチャネルＭＯＳトランジスタを使用しているが、ＮチャネルＭＯＳトランジスタの代わりにＰチャネルＭＯＳトランジスタを使用し、ゲートに印加する信号（制御信号）の１と０とを反転させるようにしてもよく、これによって、ビット順入れ換えブロック３０ａにおける動作と同様の動作を実現することができる。

【００４７】さらに、ＰチャネルＭＯＳトランジスタとＮチャネルＭＯＳトランジスタとの両者を用いて、データバス２０の配線の１つと、マイクロプロセッサ４０のデータバス端子４０ｔの１つの配線とを接続し、ＰチャネルＭＯＳトランジスタのゲートには、ＮチャネルＭＯＳトランジスタのゲートに印加する制御信号の反転信号を印加してもよく、これによっても、ビット順入れ換えブロック３０ａにおける動作と同様の動作を実現することができる。

【００４８】また、ビット順入れ換えブロック３０ａに使用されている各ＭＯＳトランジスタの制御信号を、メモリ１０の所定領域に格納するようにしてもよい。

【００４９】図７は、ビット順入れ換えブロック３０ａに使用されている各ＭＯＳトランジスタの制御信号が、

メモリ１０に格納されている例を示す図である。

【００５０】メモリ１０の０番地のビット７には、７－０の制御信号（マイクロプロセッサ４０側の配線Ｄ７とデータバス２０側の配線Ｄ０との断続を制御する制御信号）が格納され、ビット６には６－０の制御信号（マイクロプロセッサ４０側の配線Ｄ６とデータバス２０側の配線Ｄ０との断続を制御する制御信号）が格納され、以下、上記と同様にして、６４ビットの制御信号が、メモリ１０の０番地から７番地に格納されている。

【００５１】図８は、図２に示したビット順の入れ換えをするために、ビット順入れ換えブロック３０ａに供給する制御信号を示す図である。

【００５２】上記制御信号は、メモリ１０の０番地から７番地に格納されているデータであり、その０番地から順に、００００１０００、００１００００、０１００００００、００００００１０、００００１００、１０００００００、００１００００、００００００１が格納されている。

【００５３】図９は、図７に示すトランジスタの制御信号を使用して、ビット順入れ換えブロック３０ａを制御する場合に必要なメモリセルＭＣの具体例と、メモリセルＭＣとトランジスタとの接続関係を示す図である。

【００５４】メモリ１０の各ビット内の所定のノードと、対応するトランジスタのゲート電極とを接続することによって、所定のトランジスタをオンさせ、ビット順の入れ換えを可能にする。なお、ここでは、メモリセルＭＣとして１ポートのＳＲＡＭを示してあるが、１ポートのＳＲＡＭの代わりに、２ポートＳＲＡＭ、ＥＥＰＲＯＭ、ＲＯＭ等を使用してもよく、このようにしても、１ポートのＳＲＡＭを使用した場合の効果と同様の効果を得ることができる。また、特にＳＲＡＭを使用し、そのＳＲＡＭに書き込むデータを変更すればビット順の入れ換えが可能であるので、所定の時点で、上記ＳＲＡＭに書き込まれているデータを書き換えることによって、ビット順の入れ換えの順番を変更することも可能である。

【００５５】図１０は、上記実施例において、メモリ１０に格納されるビット順変換プログラムの作成法の一例を示す図である。

【００５６】プログラムＰ１は、従来のマイクロプロセッサ４で動作可能なプログラムであり、プログラムＰ２は、上記実施例におけるマイクロプロセッサ４０で動作可能なプログラムであり、プログラムＰは、プログラムＰ１をプログラムＰ２に変換するビット順変換プログラムである。つまり、同一ワード内のビット位置を変換するビット順変換プログラムＰによって、元のプログラムＰ１からプログラムＰ２を作成する。このビット順変換プログラムＰを格納するマスクＲＯＭ６１を作成し、このマスクＲＯＭ６１をマイクロプロセッサ４０と接続する。

【００５７】また、ＲＯＭライタを用い、上記変換後のプログラムＰ２をＥＰＲＯＭ６２やＥＥＰＲＯＭ６３に書き込み、これを上記実施例のマイクロプロセッサ４０と接続するようにしてもよい。

【００５８】さらに、上記変換後のプログラムＰ２を読込可能なローダープログラム、またはマイクロプロセッサ４０で動作しているローダープログラムを使用し、上記変換後のプログラムＰ２をＲＡＭに読み込めば、上記変換後のプログラムＰ２を実行することができる。さらに、ローダープログラムまたはモニタプログラムがビット順変換機能を備えたものであれば、元のプログラムＰ１を直接変換し、この変換後のプログラムＰ２をＲＡＭにロードし、マイクロプロセッサ４０で実行するようにしてもよい。

【００５９】図１１は、上記実施例において、ビット順変換プログラムＰによるビット順変換動作を示すフローチャートである。

【００６０】上記ビット順変換プログラムＰは、所定の記録媒体に記録され、この記録されたビット順変換プログラムを、マイクロプロセッサ４０とは異なるコンピュータで実行するものである。上記所定の記録媒体として、図１０に示すマスクＲＯＭ６１、ＥＰＲＯＭ６２、ＥＥＰＲＯＭ６３等と、図示しないＦＤ、ＣＤ－ＲＯＭ等との２種類が考えられる。

【００６１】まず、ビット順変換前のプログラムである元のプログラムＰ１を１バイトを読み込み（Ｓ１）、読み込んだ１バイトの中でビット位置の入れ換えを行う。ここでは、図２に示すビット順入れ換えブロック３０におけるビット順変換と同じ順で変換する場合を示してある（Ｓ２）。すなわち、ビット７のデータをビット５に変更し、ビット６のデータをビット２に変更し、ビット５のデータをビット１に変更し、ビット４のデータをビット６に変更し、ビット３のデータをビット０に変更し、ビット２のデータをビット４に変更し、ビット１のデータをビット３に変更し、ビット０のデータをビット７に変更し、これによって、新しいデータを１バイト作成する。次に、このデータを書き出し（Ｓ３）、ファイル全体の処理が終わっていなければ（Ｓ４）、さらに１バイトのデータについて、上記と同様の処理（Ｓ１～Ｓ３）を実行する。

【００６２】上記実施例において、ビット順変換プログラムＰの代わりに、ローダーまたはモニタプログラムを使用するようにしてもよい。

【００６３】つまり、上記マスクＲＯＭ６１、ＥＰＲＯＭ６２、ＥＥＰＲＯＭ６３等と、図示しないＦＤ、ＣＤ－ＲＯＭ等は、ビット順変換前のデータまたはプログラムを所定バイト、読み込む読み込み手順と、上記読み込んだ所定バイトの中でビット位置の入れ換えを行うビット位置入れ換え手順と、上記ビット位置の入れ換えが行われたデータまたはプログラムを書き出す書き出し手順

とをコンピュータに実行させるマイクロプロセッサ動作解析防止プログラムが記録されているコンピュータ読み取り可能な記録媒体の例である。

【００６４】図１２は、本発明の第２の実施例であるマイクロプロセッサシステムＭＳ２を示す図である。

【００６５】マイクロプロセッサシステムＭＳ２は、メモリ１０と、データバス２０と、マイクロプロセッサ４１とを有するものである。マイクロプロセッサ４１は、マイクロプロセッサコア４１ｃと、ビット順入れ換えブロック３０とを有するものである。

【００６６】第１の実施例であるマイクロプロセッサシステムＭＳ１では、データバス２０とマイクロプロセッサ４０のデータバス端子４０ｔとの間に、ビット順入れ換えブロック３０を接続してあるが、マイクロプロセッサシステムＭＳ２では、マイクロプロセッサ４１内にビット順入れ換えブロック３０を配置し、マイクロプロセッサコア４１ｃとデータバス端子４１との間でビット順が入れ換えられ、データバス端子１０ｔとマイクロプロセッサ４１のデータバス端子４１ｔとは、同じビット順で１：１に接続されている。

【００６７】図１３は、マイクロプロセッサシステムＭＳ２に使用されているビット順入れ換えブロック３０の具体例を示す図である。

【００６８】マイクロプロセッサコア４１ｃのデータバス端子４１ｃｔの配線Ｄ７は、ビット順入れ換えブロック３０を介して、マイクロプロセッサ４１のデータバス端子４１ｔの配線Ｄ５に接続されている。

【００６９】このデータバス端子４１ｔの配線Ｄ５は、データバス２０の配線Ｄ５を介して、メモリ１０のデータバス端子１０ｔの端子Ｄ５に接続されている。すなわち、マイクロプロセッサコア４１ｃのデータバス端子４１ｃｔの配線Ｄ７は、メモリ１０の配線Ｄ５に接続されている。

【００７０】上記と同様に、マイクロプロセッサコア４１ｃの配線Ｄ６は、マイクロプロセッサ４１のデータバス端子４１ｔの配線Ｄ２に接続され、これはデータバス２０の配線Ｄ２を介して、メモリ１０のデータバス端子１０ｔの配線Ｄ２に接続されている。また、上記と同様に、マイクロプロセッサコア４１ｃの各端子が、メモリ１０のデータバス端子１０ｔの所定の端子に接続されている。

【００７１】上記のようにすると、マイクロプロセッサコア４１ｃのデータバス端子４１ｃｔと、メモリ１０のデータバス端子１０ｔとの間で、図２に示す接続と同等の接続を実現することができる。また、マイクロプロセッサシステムＭＳ２におけるビット順入れ換えブロック３０として、図５に示すビット順入れ換えブロック３０、図６に示すビット順入れ換えブロック３０ａを使用することができる。

【００７２】図１４は、従来のマイクロプロセッサの内部におけるマイクロプロセッサコアと双方向バッファとを示す図である。

【００７３】マイクロプロセッサ４１では、マイクロプロセッサ４１内部の論理回路とメモリとを有するマイクロプロセッサコア４１ｃと、その端子を外部と接続する入力バッファ、出力バッファ、双方向バッファ等とによって構成されている。図１４では、説明に必要な双方向バッファのみを示してある。上記双方向バッファは、通常、トライステート出力バッファと入力バッファとで構成され、入力端子Ｉは、トライステート出力バッファを介して入出力端子ＩＯに接続され、入出力端子ＩＯは、入力バッファを介して出力端子Ｏに接続されている。また、制御端子ＩＯＣＯＮＴによって、トライステートバッファは、出力またはハイインピーダンス状態に制御されている。入力端子Ｉは、マイクロプロセッサコア４１ｃのデータ出力端子に接続され、出力端子Ｏは、マイクロプロセッサコア４１ｃのデータ入力端子に接続され、入出力端子ＩＯは、マイクロプロセッサ４１のデータバス端子４１ｔに接続されている。

【００７４】図１５は、図１４に示すマイクロプロセッサ４１において、図１３に示す実施例を実現する具体的な回路を示す図である。

【００７５】図１５では、双方向バッファとマイクロプロセッサ４１のデータバス端子４１ｔとの間に、ビット順入れ換えブロック３０を置いたものである。

【００７６】図１６は、図１４に示すマイクロプロセッサ４１において、図１３に示す実施例を実現する別の具体的な回路を示す図である。

【００７７】図１６では、双方向バッファとマイクロプロセッサコア４１ｃとの間に、ビット順入れ換えブロック３０を置いたものである。

【００７８】図１５、図１６のいずれの方法によっても、図２で示した場合と同様のビット順入れ換えが可能になる。

【００７９】図１７は、本発明の第３の実施例であるマイクロプロセッサシステムＭＳ３を示す図である。

【００８０】マイクロプロセッサシステムＭＳ３は、４つのビット順入れ換えブロック３１、３２、３３、３４を有する。つまり、マイクロプロセッサ４２の内部にビット順入れ換えブロック３１が設けられ、マイクロプロセッサ４２のデータバス端子４２ｔとデータバス２０との間にビット順入れ換えブロック３２が設けられ、データバス２０とメモリ１１のデータバス端子１１ｔとの間にビット順入れ換えブロック３３が設けられ、メモリ１１の内部にビット順入れ換えブロック３４が設けられている。

【００８１】図１８は、マイクロプロセッサシステムＭＳ３におけるビット順の入れ換えをより具体的に示す図である。

【００８２】ビット順入れ換えブロック３１～３４にお

いて、それぞれ個別にビット順を入れ換え、マイクロプロセッサコア４２ｃのデータバス端子４２ｃｔとメモリコア１１ｃのデータバス端子１１ｃｔとの間で、最終的に、図２に示すビット順の入れ換えと同様のビット順の入れ換えを行っている。

【００８３】ここで、ビット順入れ換えブロック３１～３４のそれぞれの構成として、ビット順入れ換えブロック３０、３０ａの構成を採用してもよく、また、各種ビット順を入れ換える他の構成を採用するようにしてもよい。

【００８４】また、マイクロプロセッサシステムＭＳ３において、４つのビット順入れ換えブロック３１～３４のうちで、少なくとも１つのビット順入れ換えブロックを使用するようにしてもよい。この場合、各ブロック内の入れ換えを適切にすることによって、任意の入れ換えが可能になる。ただし、ビット順入れ換えブロック３３のみで構成した場合、またはビット順入れ換えブロック３４のみで構成した場合、またはビット順入れ換えブロック３３と３４とで構成した場合、データバス２０上におけるデータは、ビット順が正しく並べ替えられたデータになるので、メモリ１１内のデータ観測を阻止することができるが、データバス２０を観測されると、正しいプログラムを読み出されてしまう。

【００８５】

【発明の効果】本発明によれば、メモリの内容またはデータバス上のデータを読み取られたとしても、第三者がプログラムを解析することが困難であり、ＩＣカード等のプロセッサのセキュリティを向上させることができるという効果を奏する。

【図面の簡単な説明】

【図１】本発明の第１の実施例であるマイクロプロセッサシステムＭＳ１を示す図である。

【図２】上記実施例中のビット順入れ換えブロック３０の具体例を示す図である。

【図３】上記実施例におけるメモリ１０に格納すべきデータの例を示す図である。

【図４】上記実施例において、メモリ１０のデータバス端子１０ｔにおけるプログラムのビット順と、マイクロプロセッサ４０のデータバス端子４０ｔにおけるプログラムのビット順とが、どのように変換されているかを具体的に示す図である。

【図５】上記実施例中のビット順入れ換えブロック３０の具体例を示す図である。

【図６】ビット順入れ換えブロック３０の代わりに使用することができるビット順入れ換えブロック３０ａの構成を示す図である。

【図７】ビット順入れ換えブロック３０ａに使用されている各ＭＯＳトランジスタの制御信号が、メモリ１０に格納されている例を示す図である。

【図８】ビット順入れ換えブロック３０ａを使用し、図２に示したビット順の入れ換えをするために、ビット順入れ換えブロック３０ａに供給する制御信号を示す図である。

【図９】図７に示すトランジスタの制御信号を使用して、ビット順入れ換えブロック３０ａを制御する場合に必要なメモリセルＭＣの具体例と、メモリセルＭＣとトランジスタとの接続関係を示す図である。

【図１０】上記実施例において、メモリ１０に格納されるビット順変換プログラムの作成法の一例を示す図である。

【図１１】上記実施例において、ビット順変換プログラムＰによるビット順変換動作を示すフローチャートである。

【図１２】本発明の第２の実施例であるマイクロプロセッサシステムＭＳ２を示す図である。

【図１３】マイクロプロセッサシステムＭＳ２に使用されているビット順入れ換えブロック３０の具体例を示す図である。

【図１４】従来のマイクロプロセッサの内部におけるマイクロプロセッサコアと双方向バッファとを示す図である。

【図１５】図１４に示すマイクロプロセッサ４１において、図１３に示す実施例を実現する具体的な回路を示す図である。

【図１６】図１４に示すマイクロプロセッサ４１において、図１３に示す実施例を実現する別の具体的な回路を示す図である。

【図１７】本発明の第３の実施例であるマイクロプロセッサシステムＭＳ３を示す図である。

【図１８】マイクロプロセッサシステムＭＳ３におけるビット順の入れ換えをより具体的に示す図である。

【図１９】従来のマイクロプロセッサシステムＭＳの構成の一例を示す図である。

【図２０】上記従来例におけるマイクロプロセッサのデータバス端子とメモリのデータバス端子との接続を示す図である。

【図２１】上記従来例におけるメモリ１の内容を示す図である。

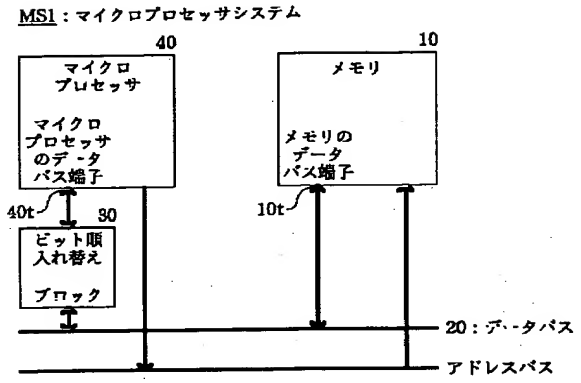
【符号の説明】

ＭＳ１～ＭＳ３…マイクロプロセッサシステム、
１０…メモリ、
１０ｔ…メモリのデータバス端子、
２０…データバス、
３０、３１ａ、３１、３２、３３、３４…ビット順入れ換えブロック、
４０、４１、４２…マイクロプロセッサ、
４０ｔ、４１ｔ、４２ｔ…マイクロプロセッサのデータバス端子、
４１ｃ、４２ｃ…マイクロプロセッサコア、
Ｐ…ビット順変換プログラム、

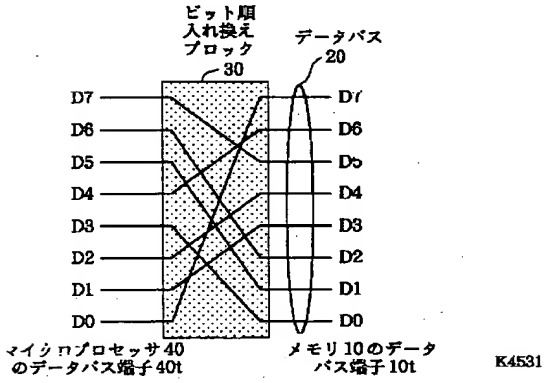
Ｐ１…ビット順変換前のプログラム、

Ｐ２…ビット順変換後のプログラム。

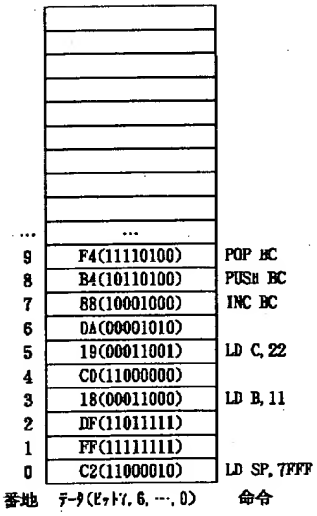
【図１】



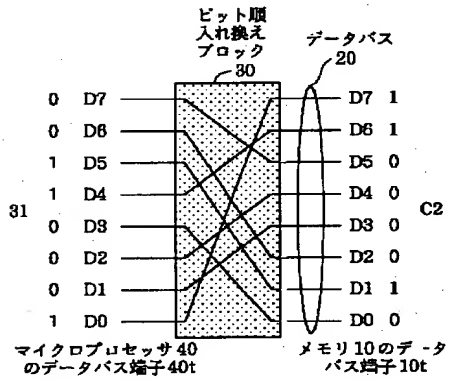
【図２】



【図３】



【図４】

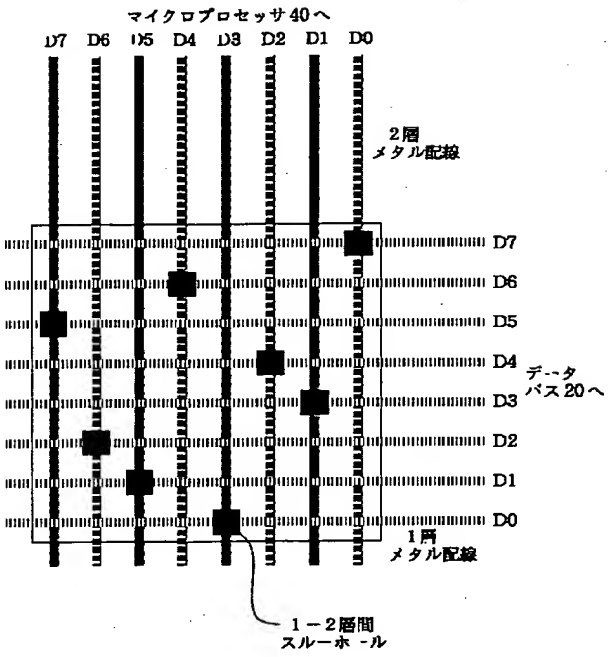


K4531

K4531

【図5】

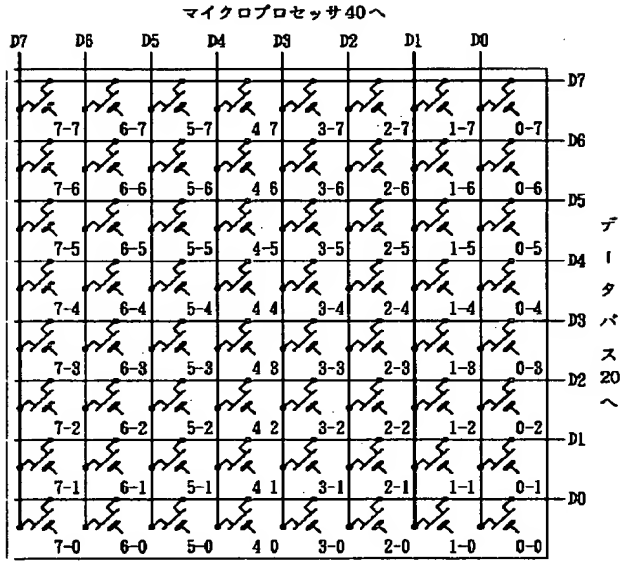
30：ビット順入れ換えブロック



K4531

【図6】

30a：ビット順入れ換えブロック



K4531

【図7】

ビット順入れ換えブロック 30a を制御する制御信号

	ビット7							ビット0
7	7－7	6－7	5－7	4－7	3－7	2－7	1－7	0－7
6	7－6	6－6	5－6	4－6	3－6	2－6	1－6	0－6
5	7－5	6－5	5－5	4－5	3－5	2－5	1－5	0－5
4	7－4	6－4	5－4	4－4	3－4	2－4	1－4	0－4
3	7－3	6－3	5－3	4－3	3－3	2－3	1－3	0－3
2	7－2	6－2	5－2	4－2	3－2	2－2	1－2	0－2
1	7－1	6－1	5－1	4－1	3－1	2－1	1－1	0－1
0	7－0	6－0	5－0	4－0	3－0	2－0	1－0	0－0

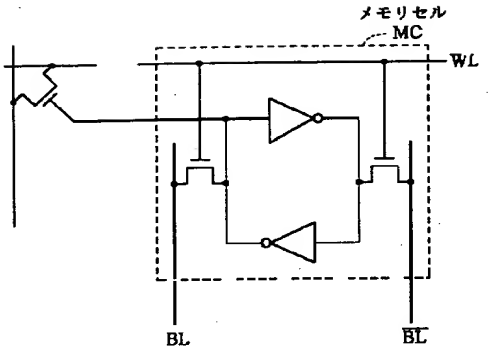
【図8】

ビット順入れ換えブロック 30a を制御する制御信号

7	00000001
6	00010000
5	10000000
4	00000100
3	00000010
2	01000000
1	00100000
0	00001000

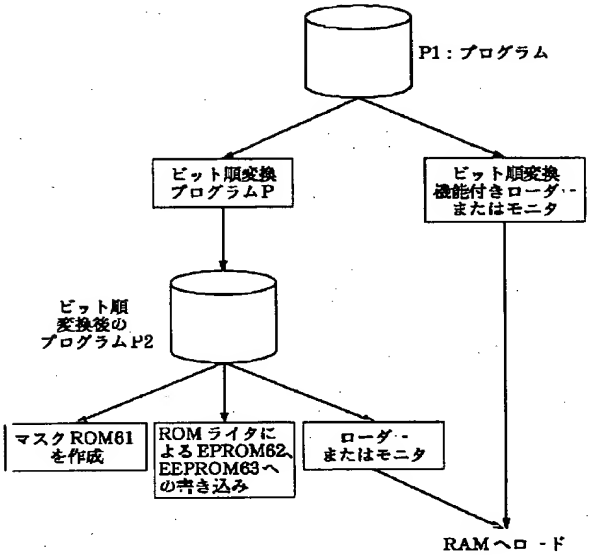
K4531

【図9】



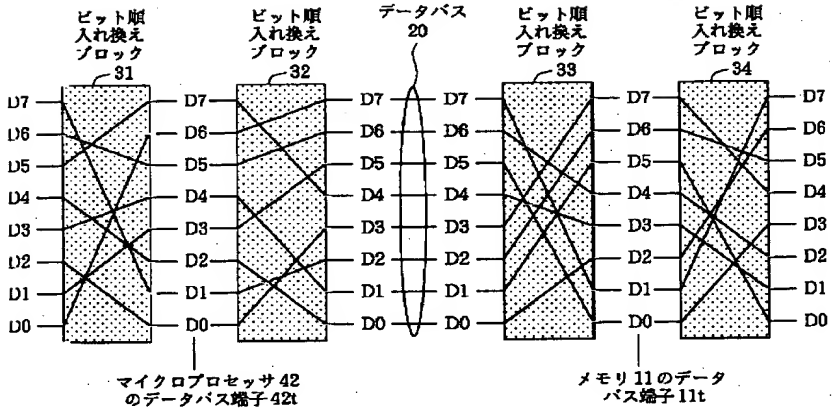
K4531

【図10】



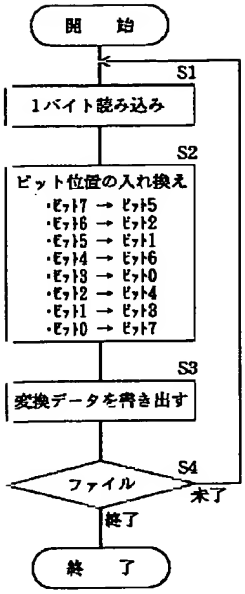
K4531

【図18】



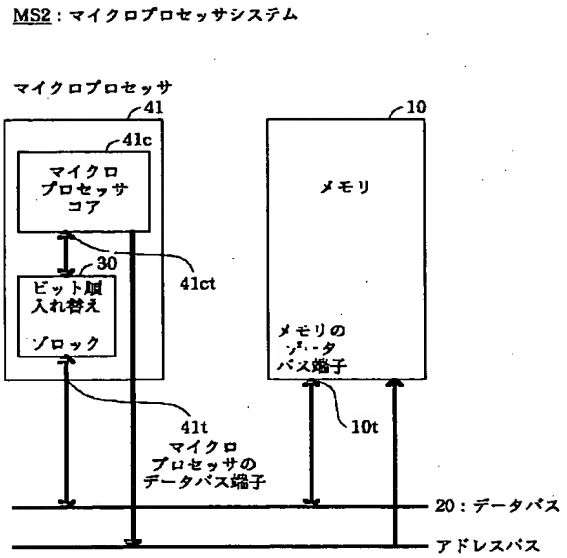
K4531

【図11】



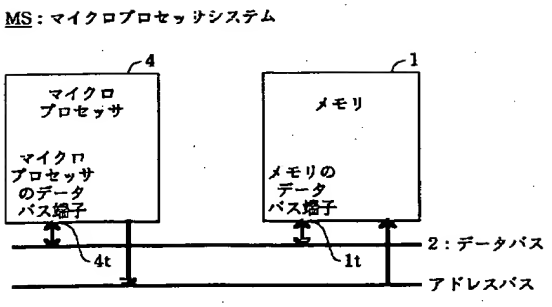
K4531

【図12】

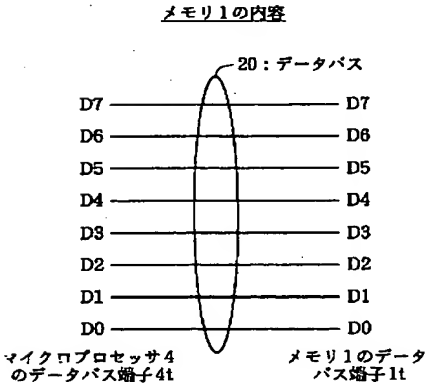


K4531

【図19】

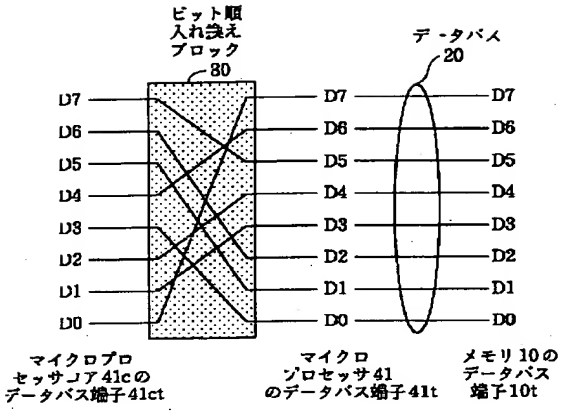


【図20】

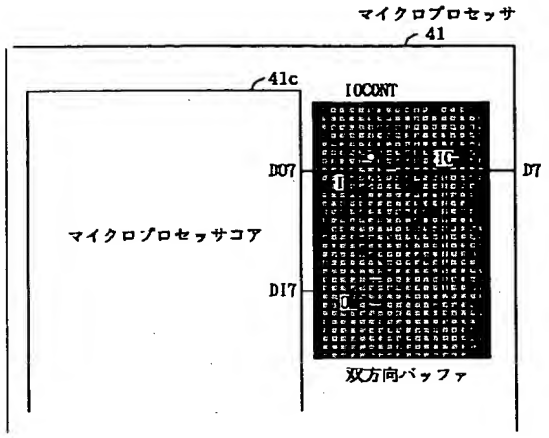


K4531

【図13】



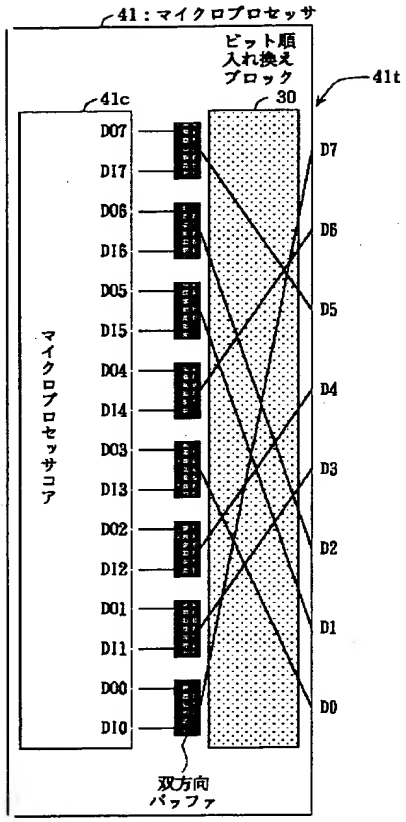
【図14】



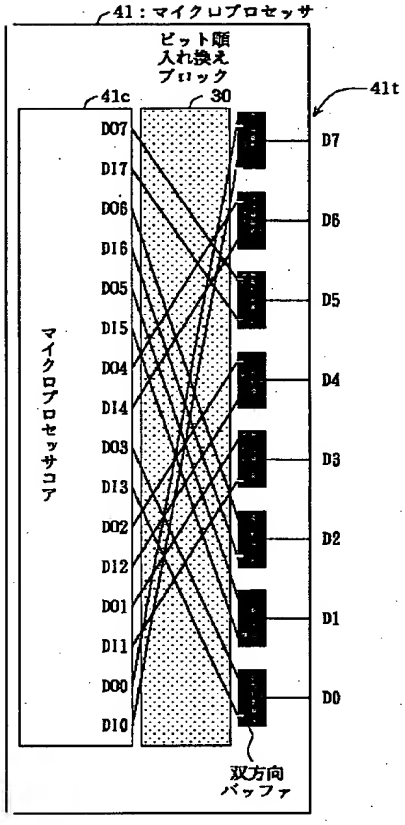
K4531

K4531

【図15】

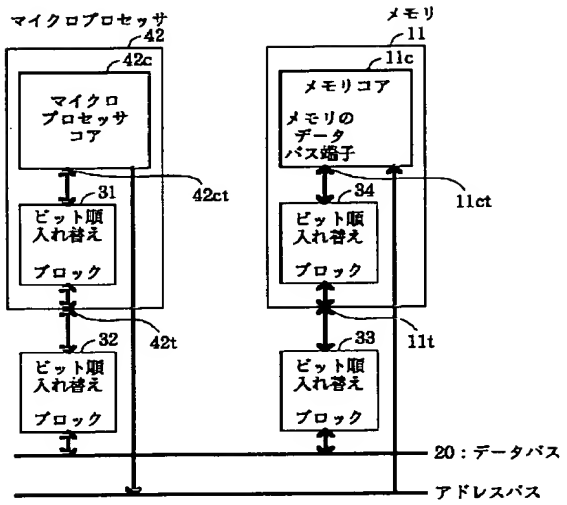

41：マイクロプロセッサ
ビット順
入れ換え
ブロック
41t
41c
30
DO7
DI7
DO6
DI6
DO5
DI5
DO4
DI4
DO3
DI3
DO2
DI2
DO1
DI1
DO0
DI0
D7
D6
D5
D4
D3
D2
D1
D0
マイクロプロセッサコア
双方向
バッファ
K4531

【図16】


41：マイクロプロセッサ
ビット順
入れ換え
ブロック
41t
41c
30
DO7
DI7
DO6
DI6
DO5
DI5
DO4
DI4
DO3
DI3
DO2
DI2
DO1
DI1
DO0
DI0
D7
D6
D5
D4
D3
D2
D1
D0
マイクロプロセッサコア
双方向
バッファ
K4531

【図17】

MS3：マイクロプロセッサシステム



K4531

【図21】

メモリ1の内容

番地	データ(ビット7, 6, …, 0)	命令
…	…	
9	D5(11010101)	POP BC
8	C5(11000101)	PUSH BC
7	03(00000011)	INC BC
6	22(00100010)	
5	0E(00001110)	LD C, 22
4	11(00010001)	
3	06(00000110)	LD B, 11
2	7F(01111111)	
1	FF(11111111)	
0	31(00110001)	LD SP, 7FFF

K4531